体の直積構造を利用したBoolean Grobner Basisの並列計算アルゴリズムについて (数式処理における理論と応用の研究)

AUTHOR(S):

佐藤, 洋祐; 三橋, 元洋

数理解析研究所講究録
1085巻 1999年 25-33

体の直積構造を利用した Boolean Gröbner Basis の並列計算アルゴリズムについて

立命館大学理工学部 佐藤洋祐 *
立命館大学理工学部 三橋元洋 †

1 はじめに

係数環が commutative Von Neumann regular ring である多項式環において、独特の M-reduction を用いることでグレブナー基底を計算することができる ([S 88,S 90,W 89]). この方法は、[S 95] の集合制約ソルバーにおけるグレブナー基底計算アルゴリズムとして実装されている. 一方、任意の commutative Von Neumann regular ring は体の直積のなす環の部分環と同型になることが知られており ([SW 75])、この直積構造があらかじめわかっている場合は、各成分の体上の多項式環におけるグレブナー基底を計算することで、元の環におけるグレブナー基底を求めることができる ([W 89, Sa 98, Sb 98]). この方法は並列計算が利用できる環境においては特に有効である. さて、上記の集合制約ソルバーで扱う係数環は本質的に有限ブール環なので、有限体 $GF(2)$ の直積と同型になり、その構造も容易に記述することができる. したがって、独特の M-reduction を用いるアルゴリズムよりも、体の直積構造を利用した並列アルゴリズムの方が有効であると予想される. 本論文では、上記の2つのアルゴリズムを用いておこなったグレブナー基底の計算に関するわれわれの実験結果について報告する. 以下、2節において基礎となる理論を述べる. ほとんどの結果は一般の commutative Von Neumann regular ring においても成り立つが、記述がやや複雑になるので、ブール環だけを対象とする. われわれの実験結果については3節で述べる.

*ysato@theory.cs.ritsumei.ac.jp
†mituhasi@theory.cs.ritsumei.ac.jp

2 ブール環とグレブナー基底

単位元をもつ可換環 $\mathbf{B}$ が以下の性質を持つとき、これをブール環とよぶ.

$$\forall x \in \mathbf{B}\ x^2 = x$$

ストーンの表現定理を用いると、$\mathbf{B}$ から $\prod_{I \in St(\mathbf{B})} \mathbf{B}/I$ の中への同型写像 Φ が

$$\Phi(x) = \prod_{I \in St(\mathbf{B})} [x]_I$$

で得られる. ここで、$St(\mathbf{B})$ は $\mathbf{B}$ の極大イデアル全体の集合を表す.
体 $\mathbf{B}/I$ は $GF(2)$ と同型であるので、$\mathbf{B}$ は $GF(2)$ の直積のなす環の部分環と同型であることがわかる. $\mathbf{B}$ が有限ブール環の場合、 $St(\mathbf{B})$ は有限なので、直積は有限個であり、さらに Φ は上への写像になるので、$\mathbf{B}$ は $GF(2)$ の有限個の直積のなす環と同型になる.

以下では、ブール環 $\mathbf{B}$ 上の多項式環において作業をおこなう. 単項を表す記号としてギリシャ文字 α、β、γ 等を、ブール環 $\mathbf{B}$ の要素を表す記号として a、b、c 等を、多項式を表す記号として f、g、h 等を用いる. また、単項上のアドミシブル順序を 1 つ固定し、これによる f の最大の単項を $lt(f)$、その係数を $lc(f)$、最大の単項式すなわち $lc(f)lt(f)$ を $lm(f)$ 、$f - lm(f)$ を $rm(f)$ で表す.

定義 1 (モノミアルリダクション) 多項式 $f = a\alpha + g$*(ただし* $lm(f) = a\alpha$*)* にたいして、f によるモノミアルリダクション $\rightarrow_f$ を以下で定義する.

$$b\alpha\beta + h \rightarrow_f b\alpha\beta + h + ba\beta(\alpha + g)\ \text{(ただし、}ab \neq 0\text{)}$$

定義 2 (ブール閉) 多項式 f が、$lc(f)f = f$ をみたすとき、f はブール閉であるという. $lc(f)f$ を f のブール閉包とよび、$bc(f)$ で表す.*(注意 任意の多項式のブール閉包はブール閉である.)*

定理 3 F をブール閉な多項式の集合とすると、$\overset{*}{\leftrightarrow}_F$ による同値関係とイデアル (F) による同値関係は一致する.

グレブナー基底の定義には、いろいろな方法があるが、上のモノミアルリダクションによって以下のように定義する.

定義 4 (グレブナー基底) 多項式の有限集合 G が以下の条件をみたすとき、G はグレブナー基底であるとよばれる.

・ $\overset{*}{\leftrightarrow}_G$ による同値関係とイデアル (G) による同値関係が一致する.
・ $\rightarrow_G$ はこの同値関係の完備化システムである. すなわち、任意の多項式 f、g にたいして、$f \equiv g \Longleftrightarrow f\downarrow_G = g\downarrow_G$.

定義 5 (既約グレブナー基底) グレブナー基底 G にたいし、G の任意の要素 f が自分以外の G の要素によるモノミアルリダクションによって書き換えられないとき、G を**既約グレブナー基底**とよぶ.

定理 6 G を既約グレブナー基底とするとき、G のすべての要素はブール閉な多項式である.

定義 7 (正規グレブナー基底) 既約グレブナー基底 G がさらに以下の性質をもつとき、G を**正規グレブナー基底**とよぶ.
・ G の二つの要素で、最大単項が一致するものはない

正規グレブナー基底は次の重要な性質をもつ.

定理 8 正規グレブナー基底はユニークに定まる. すなわち、$(G) = (G')$ なる正規グレブナー基底 G と G' は一致しなければならない.

さて、上に述べたように、任意のブール環 $\mathbf{B}$ は $GF(2)$ の直積 $GF(2)^S$ のなす環の部分環に同型になる. この同型写像 ϕ を 1 つ固定し、これを用いて、ブール環 $\mathbf{B}$ における多項式 f にたいして、その $i(\in S)$ 成分 f_i を、f のすべての係数 a を $\phi(a)$ でおきかえて得られる $GF(2)$ 上の多項式と定義する. $\mathbf{B}$ 上の多項式の集合 F にたいしても、$\{f_i | f \in F\}$ を F_i で表す. これにたいし、次の定理がなりたつ.

定理 9 (重要定理) ブール閉な多項式の集合 G にたいして、以下の条件は同値になる.
・ G は既約グレブナー基底である.
・ S の各要素 i にたいして、G_i は既約グレブナー基底である.

3 実験結果

ブール環の直積構造がわかっている場合、グレブナー基底の計算は、定理 9 によって $GF(2)$ 上の多項式環におけるグレブナー基底の計算に還元される. 各成分 G_i の計算は全く独立におこなわれるので、並列計算が容易に実現可能になる. 以下に、われわれがおこなった実験結果について述べる.

ブール環 $\mathbf{B}$ として、A を 加算無限集合として、
$\mathbf{B} = \{P | P \subseteq A \text{ and } P \text{ is a finite set or a complement of a finite set}\}$ で定義されるブール環を用いた. これは有限ブール環ではないが、実際のグレブナー基底の計算では、これの有限部分環のみを用い、直積構造も自明である. 対象領域がブール環であるので、多項式環 $\mathbf{B}[X_1, X_2, \ldots, X_n]$ ではなく、剰余環 $\mathbf{B}[X_1, X_2, \ldots, X_n]/(X_1^2+X_1, X_2^2+X_2, \ldots, X_n^2+X_n)$ における正規グレブナー基底 (われわれはこれを Boolean Gröbner Basis とよんでいる [S 95].) の計算をおこなった.

実験データの紹介をする前に、定理 9 を用いてどのような計算をするのか、まず簡単な例で説明する. $a, b \in A$ として、

$$((\tilde{}\{a,b\}) * x * y + \{a\} * x + y + \{b\}, x * y + \{a\} * y + x + \{a,b\})$$

の $\mathbf{B}[x,y]/(x^2+x, y^2+y)$ におけるグレブナー基底の計算には $\mathbf{B}$ の有限部分環 $\{0, 1, \{a\}, \{b\}, \{a,b\}, \tilde{}\{a,b\}, \tilde{}\{a\}, \tilde{}\{b\}\}$ の要素のみが現れるので、この部分環における計算を考えればよい.

この有限ブール環のアトミックな要素は $\{a\}$、$\{b\}$、$\tilde{}\{a,b\}$ の 3 つなので、この部分環は $GF(2)^3$ と同型になる. この同型写像を ϕ とおく. ただし $\phi(\{a\}) = (1,0,0), \phi(\{b\}) = (0,1,0), \phi(\tilde{}\{a,b\}) = (0,0,1)$ とする. このとき、多項式 $(\tilde{}\{a,b\}) * x * y + \{a\} * x + y + \{b\}, x * y + \{a\} * y + x + \{a,b\}$ の ϕ による像は $GF(2)^3$ 上の多項式 $(0,0,1) * x * y + (1,0,0) * x + (1,1,1) * y + (0,1,0), (1,1,1) * x * y + (1,0,0) * y + (1,1,1) * x + (1,1,0)$ となる.
G を $GF(2)^3[x,y]/(x^2+x, y^2+y)$ における、これの既約グレブナー基底とすると、定理 9 によれば、

G_1 は $GF(2)[x,y]/(x^2+x, y^2+y)$ における $x+y, x*y+y+x+1$ の既約グレブナー基底、
G_2 は $GF(2)[x,y]/(x^2+x, y^2+y)$ における $y+1, x*y+x+1$ の既約グレブナー基底、
G_3 は $GF(2)[x,y]/(x^2+x, y^2+y)$ における $x*y+y, x*y+x$ の既約グレブナー基底
である. これを計算すると、それぞれ $\{y+1, x+1\}$、$\{1\}$、$\{y+x\}$ になる. よって $G = \{(1,0,0)*(y+1), (1,0,0)*(x+1), (0,1,0), (0,0,1)*(y+x)\}$ とおくと、G は求める既約グレブナー基底になる. このままでは G は正規ではないので、最大単項の同じものを 1 つに足し合わせて正規グレブナー基底 $\{(1,0,1)*y+(0,0,1)*x+(1,0,0), (1,0,0)*(x+1), (0,1,0)\}$ を得る. これの ϕ による逆像 $\{\tilde{}\{b\} * y + \tilde{}\{a,b\} * x + \{a\}, \{a\} * (x+1), \{b\}\}$ が最終的に求める正規グレブナー基底である.

以下に実験結果を述べる. [S 95] の KLIC(並列論理型言語) で記述されたグレブナー基底計算プログラムによる計算結果をあげているが、参考のために ASIR の `gr_mod` による計

算結果もあげている. 使用した計算機は PentiumPro200Mhz、OS は FreeBSD である. 以下の例では最初のリストの多項式によって生成されるイデアルの正規グレブナー基底の計算に要した時間が記されている.
いずれも 20 変数 x1,x2,x3,x4,x5,x6,x7,x8,x9,x10,y1,y2,y3,y4,y5,y6,y7,y8,y9,y10 を含む. アトミックな要素は例 1 が a,b,c,d,e,f,g,h,i,j,k の 1 1個、例 2、3 が a,b,c,d,e,f,g の 7 個である. 単項順序は全次数逆辞書式を用いた. 尚、集合を表す記号 { 、 } として [、] を用いている.

例 1.

```
[
[a,b,d]*x1*x2*x3*y1*y4*y7+[f,h]*x4*y4*y7*y10+[b]*x6*x10,
[c,j,a]*x2*x5+[d,f]*x4*x5*x6+[a,b,h]*x4*x8*x10+[b,c,k]*x6*x7*x10,
[b,d]*x4*y5+[a,c]*x3*x10+[b,f,g]*y4+[a,b,d,g]*x5*[f]*y9,
[c,g,i]*x2*x4*x5*y3*y6*y9+[a,b,c]*x3*x4*y1*y4*y8+[b,f,g]*x4*x7*y6*y8+
   [a,b,d,g]*x5*x9*x10*y5*y7*y8,
[b,f]*x1*x3*x5*y2*y4+[b,c,g,k]*x2*x5*y7*y9+[d,f,g,a,h]*x4*y2*y3*y6,
[a]*x6*y1*y3*y6+[b,e,f]*x5*x9*y7+[f,i,k]*x8*x10*y4*y8,
[b]*x1*y6*y8+[c,j]*x2*x8*y3+[d,k]*x3*y6*y7*y8+[a,e,i]*x4*x6*x9*y3*y7+
   [f,k,j]*x5*x10*y10+[g,h]*x6*y2*y3*y6+[i,j,k]*x7*x8*y3*y6*y10,
[b,e]*x2*x4*x7*y4*y8+[a,g,h]*x3*x6*x7*y3*y8+[b,c]*x4*y1*y4*y7,
[d]*x3*y3+[b,c,e]*x3*x4*y4+[d,h,k,i]*x5*x6*x7*y1+[e,f,g]*x7*y2+
   [f,k]*x5*y7+[g,h,j]*x6*y3*y6,
[a,c]*x1*y2*y3+[b,e,f,g,h]*x4*x5*x9*y6+[a,b,k,i]*x2*x6*y3*y6+
   [i,j,f,h]*x7*y8*y2+[a]*x8*x9*x10*y3*y5
]
```

独自のモノミアルリダクションを用いた計算時間　29sec
各アトミック要素にたいする $GF(2)$ 上の多項式環における計算時間 (下段は ASIR による計算)

a	b	c	d	e	f	g	h	i	j	k	合計
1.3	1.4	0.1	0.1	0.1	0.4	0.2	0.2	0.4	0.1	0.4	4.7sec
0.29	0.59	0.03	0.02	0.04	0.11	0.08	0.04	0.08	0.03	0.10	1.41sec

例 2.

```
[
[a,b,d]*x1*x2*x3*y1*y4*y7+[f]*x4*y4*y7*y10+[b]*x6*x10,
```

```
[c,a]*x2*x5+[d,f]*x4*x5*x6+[a,b]*x4*x8*x10+[b,c]*x6*x7*x10,
[b,d]*x4*y5+[a,c]*x3*x10+[b,f,g]*y4+[a,b,d,g]*x5+[f]*y9,
[c,g]*x2*x4*x5*y3*y6*y9+[a,b,c]*x3*x4*y1*y4*y8+[b,f,g]*x4*x7*y6*y8+
   [a,b,d,g]*x5*x9*x10*y5*y7*y8,
[b,f]*x1*x3*x5*y2*y4+[b,c,g]*x2*x5*y7*y9+[d,f,g,a]*x4*y2*y3*y6,
[a]*x6*y1*y3*y6+[b,e,f]*x5*x9*y7+[f]*x8*x10*y4*y8,
[b]*x1*y6*y8+[c]*x2*x8*y3+[d]*x3*y6*y7*y8+[a,e]*x4*x6*x9*y3*y7+
   [f]*x5*x10*y10+[g]*x6*y2*y3*y6+[b]*x7*x8*y3*y6*y10,
[b,e]*x2*x4*x7*y4*y8+[a,g]*x3*x6*x7*y3*y8+[b,c]*x4*y1*y4*y7,
[d]*x3*y3+[b,c,e]*x3*x4*y4+[b,d]*x5*x6*x7*y1+[e,f,g]*x7*y2+[f,c]*x5*y7+
   [g,a]*x6*y3*y6,
[a,c]*x1*y2*y3+[b,e,f,g]*x4*x5*x9*y6+[a,b,c]*x2*x6*y3*y6+
   [a,d,f]*x7*y8*y2+[a]*x8*x9*x10*y3*y5
]
```

独自のモノミアルリダクションを用いた計算時間　46sec

各アトミック要素にたいする $GF(2)$ 上の多項式環における計算時間 (下段は ASIR による計算)

a	b	c	d	e	f	g	合計
4.4	8.8	0.7	0.2	0.2	0.8	0.6	15.7sec
0.24	1.26	0.07	0.03	0.03	0.12	0.09	1.84sec

例 3.

```
[
[a,b,d,g]*x1*x2*x3*y1*y4*y7+[b,e,f]*x4*y4*y7*y10+[a,d]*x6*x10,
[c,a,f]*x2*x5+[d,f]*x4*x5*x6+[a,b,e]*x4*x8*x10+[a,b,c]*x6*x7*x10,
[b,d]*x4*y5+[a,c,e,g]*x3*x10+[b,f,g]*y4+[a,b,d,g]*x5+[e,f]*y9,
[c,g]*x2*x4*x5*y3*y6*y9+[a,b,c]*x3*x4*y1*y4*y8+[b,f,g]*x4*x7*y6*y8+
   [a,b,d,g]*x5*x9*x10*y5*y7*y8,
[b,f]*x1*x3*x5*y2*y4+[b,c,g]*x2*x5*y7*y9+[d,f,g,a]*x4*y2*y3*y6,
[a]*x6*y1*y3*y6+[b,e,f]*x5*x9*y7+[b,c,f]*x8*x10*y4*y8,
[b]*x1*y6*y8+[c]*x2*x8*y3+[d]*x3*y6*y7*y8+[a,e]*x4*x6*x9*y3*y7+
   [f]*x5*x10*y10+[g]*x6*y2*y3*y6+[b,f,g]*x7*x8*y3*y6*y10,
[b,e]*x2*x4*x7*y4*y8+[a,g]*x3*x6*x7*y3*y8+[b,c,f]*x4*y1*y4*y7,
[d]*x3*y3+[b,c,e]*x3*x4*y4+[a,b,d]*x5*x6*x7*y1+[e,f,g]*x7*y2+
   [a,f,c]*x5*y7+[g,a]*x6*y3*y6,
```

```
[a,c]*x1*y2*y3+[b,e,f,g]*x4*x5*x9*y6+[a,b,c]*x2*x6*y3*y6+
   [a,d,f]*x7*y8*y2+[a,e]*x8*x9*x10*y3*y5
]
```

独自のモノミアルリダクションを用いた計算時間　176sec

各アトミック要素にたいする $GF(2)$ 上の多項式環における計算時間 (下段は ASIR による計算)

a	b	c	d	e	f	g	合計
3.1	33.1	0.1	0.1	0.1	2.1	1.1	39.7sec
0.15	2.87	0.53	0.06	0.06	0.19	0.38	4.24sec

4　おわりに

ブール環上のグレブナー基底を利用する方法は、有限領域の問題解決のための全く新しい手法であるが、この種の問題は本質的にNP-完全であり、われわれの方法はワーストケースにおいて指数オーダーであるので (剰余環で計算をするので、一般の体上のグレブナー基底の計算よりもはるかに小さいオーダーで抑えられる)、理論的にはこれ以上のものは本質的に存在しない.(P $\neq$ NP を仮定しての話であるが)

したがって、プラクティカルなアプローチが重要になる. われわれの実験結果では、体の直積構造を利用したアルゴリズムの方が、従来のアルゴリズムよりもはるかに高速であることが確かめられた. 並列計算が有効であるのは、各アトミックな要素にたいするグレブナー基底の計算の重さが分散されている場合に限るので、すべての場合に並列効果があるわけではないが、例1や2などは多少の並列効果がでる計算例になっている. 一方、例 3 の計算では並列効果はあまり期待できない. アトミックな要素の個数がもっと多い場合にどうなるか、具体的な有限領域の問題の計算実験が必要であろう.

実際に並列計算を行うために、現在 PVM を用いた KLIC の並列計算用のプログラムを開発中である. 今年度中には、[S 95] と同じ AITEC からフリーソフトウェアとして公開される予定である.

実験結果でも紹介したように、ASIR の高速なグレブナー基底の計算を利用して、われわれの Boolean Gröbner Bases の計算が可能である. これに関しても、現在開発中である.

参　考　文　献

[B 65] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. PhD thesis, Universität Innsbruck.

[B 85] Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory, chap 6 in Recent Trends in Multidimentional System Theory, N. K. Bose Ed., Reidel Publ. Comp.

[Mo 88] Möller, H.M. (1988). On the Construction of Gröbner Bases Using Syzygies *J.Symbol.Comput.* **6**, 345–359.

[S 88] Sakai, K., Sato, Y. (1988). Boolean Gröbner bases. Proceeding of LA-Symposium in winter, RIMS, Kyoto Univ., 29–40

[S 90] Sakai, K., Sato, Y., Menju, S. (1990). Boolean Gröbner bases(revised). ICOT Technical Report 613.

[S 93] 佐藤洋祐、毛受哲、相場亮 (1995). ブーリアン・グレブナー基底の Syzygy 基底による特徴付け.「情報処理学会論文誌」第 34 巻 第 7 号 pp 1549-1554.

[S 95] Sato, Y. (1995). Set Constraint Solver (a free software developed as a Research Funding Program of AITEC, Research Institute For Advanced Information Technology). http://www.icot.or.jp/AITEC/FGCS/funding/itaku-H7-index-J.html http://www.icot.or.jp/AITEC/FGCS/funding/itaku-H8-index-J.html

[Sa 96] Sato, Y. (1996). Application of Groebner basis in constraint of non-numerical domains. presented in The 2nd IMACS Conference on Applications of Computer Algebra.

[Sb 96] Sato, Y. (1996). Nonstandard Canonical Forms of Set Constraints. presented in Second International Conference on Principles and Practice of Constraint Programming Set Constraints Workshop.

[S 97] Sato, Y. (1997). Set Constraint Solver - Groebner bases for non-numerical domains -. International Symposium on Symbolic and Algebraic Computation(ISSAC 97), Poster Abstracts pp 13-14.

[Sa 98] 佐藤 洋祐 (1998). Von Neumann regular rings 上の多項式環におけるグレブナー基底について. 数理解析研究所講究録 1038「数式処理における理論と応用の研究」pp 40-48.

[Sb 98] Sato, Y. (1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. International Symposium on Symbolic and Algebraic Computation(ISSAC 98), Proceedings pp 317-321.

[SW 75] Saracino, D., Weispfenning, V. (1975). On algebraic curves over commutative regular rings, Model Theory and Algebra, a memorial tribute to A.Robinson, Springer LNM vol 498, pp 307-387.

[W 89] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings, EUROCAL '87, J.H. Davenport Ed., Springer LNCS Vol 378, 336–347.